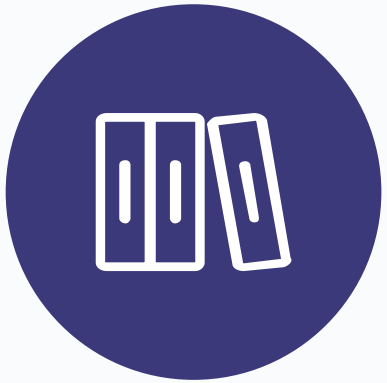


第7章 数据水印

成都信息工程大学 白杨 副教授

2024年X月X日

第7章 数据安全概述

本讲内容概要：

01 第一节—数据水印基本原理

02 第二节—数据水印嵌入

03 第三节—数据水印提取

04 第四节—数据水印应用

第7章 数据安全概述

本讲内容概要：

01 第一节—数据水印基本原理

02 第二节—数据水印嵌入

03 第三节—数据水印提取

04 第四节—数据水印应用

01 7.1.1 数据水印概述

数据水印是一种技术，用于在数据中嵌入隐蔽信息，以便在数据传播和使用过程中验证数据的来源和完整性。数据水印的原理类似于传统的图像或视频水印，但它适用于各种数据类型，如文本、图像、音频、视频和数据库等。

01 7.1.1 数据水印概述

隐蔽性（Imperceptibility）：

水印信息嵌入后不应影响原始数据的质量或可感知性。对于图像和音频，水印不应影响视觉或听觉体验；对于文本，水印不应影响可读性。

鲁棒性（Robustness）：

水印应能抵抗各种攻击和操作，如压缩、裁剪、滤波、噪声添加、格式转换等。即使数据被修改或处理，水印信息仍应保持可检测性。

容量（Capacity）：

水印技术应能够在数据中嵌入足够多的信息。容量越大，水印可以携带的信息量就越多，但通常会与隐蔽性和鲁棒性形成权衡。

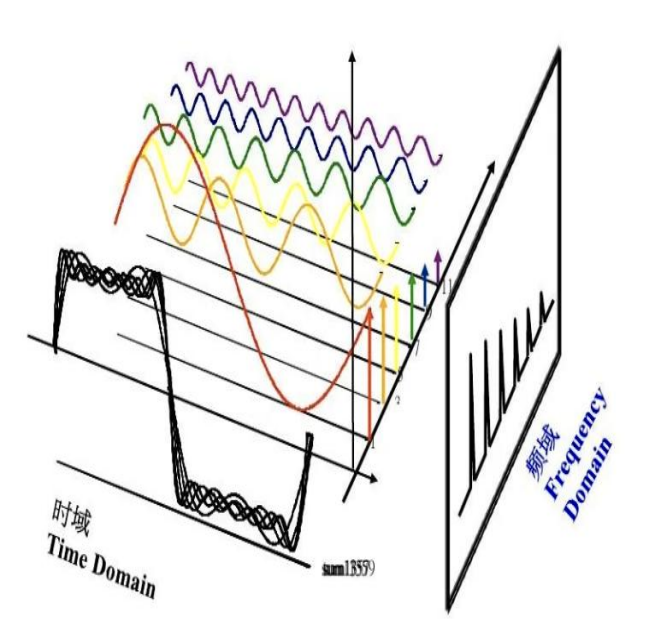
安全性（Security）：

水印应难以被恶意攻击者检测、移除或篡改。只有拥有特定密钥或算法的人才能提取或验证水印信息。

实时性（Real-time Performance）：

水印嵌入和提取过程应具有较高的效率，能够在合理的时间内完成，特别是在需要处理大量数据或实时数据时。

01 7.1.2 数据水印种类



嵌入方式分类

空域水印，频域水印

可见性分类

可见水印，不可见水印

安全性分类

强安全水印，弱安全水印，无安全水印

01 7.1.1 水印工作流程

水印信息是要嵌入到原始数据中的内容，可以是文本、图像、序列号或其他标识信息。这一步的目标是生成要嵌入的数据水印。

将生成的水印信息嵌入到原始数据中。具体的方法和步骤根据数据类型和应用场景而不同。

接收方或验证方从接收到的数据中检测或提取水印信息，以验证数据的真实性和完整性。

第7章 数据安全概述

本讲内容概要：

01 第一节—数据水印基本原理

02 第二节—数据水印嵌入

03 第三节—数据水印提取

04 第四节—数据水印应用

02 7.2.1 水印信息预处理

信息编码

哈夫曼编码（Huffman Coding）：一种无损压缩算法，通过构建哈夫曼树，对数据进行编码。

循环冗余校验（CRC）：通过附加校验码来提高水印信息的可靠性。

伪随机序列生成：利用伪随机序列生成器，将水印信息映射为伪随机序列，增强其隐蔽性。

信息加密

对称加密：如高级加密标准、数据加密标准等。

非对称加密：如RSA算法，利用公钥和私钥进行加密和解密。

混沌加密：利用混沌系统的不可预测性，对水印信息进行加密。

信息压缩

有损压缩：如JPEG图像压缩、MP3音频压缩等。这类压缩方法在一定程度上会损失数据质量。

无损压缩：如PNG图像压缩、FLAC音频压缩等。这类压缩方法不会损失数据质量。

02 7.2.1 水印信息预处理

信息编码

文本编码：将文本信息转换为二进制形式，如 ASCII 码、UTF-8 等。这样的编码方式可以确保文本信息在数字环境中的正确表示。

图像编码：对图像水印进行编码，如使用 JPEG、PNG 等格式。通过图像编码，可以将图像水印转换为数字图像的表示形式，以便与原始图像进行合并。

音频编码：对音频水印进行编码，如使用 PCM、MP3 等格式。音频编码将音频水印转换为数字音频数据，使其可以与原始音频数据进行无缝集成。

02 7.2.1 水印信息预处理

水印信息加密

数据加密是确保水印信息安全性的重要步骤，**通过加密可以防止未经授权的访问者获取敏感信息，并保护数据的机密性和完整性。**在水印嵌入和提取过程中，数据加密可以确保水印信息的安全传输和存储，同时防止数据被篡改或损坏。加密过程中，常用的密码学算法包括 MD5、Hash、AES 等，这些算法可以对敏感数据进行加密操作，生成无法直接解析的密文数据。外部未经授权的用户只能访问到无实际意义的密文数据，而无法获取敏感数据的原始内容。同时，可以为特定需求提供解密能力，以恢复敏感数据的原始内容。

通过数据加密，可以有效保护水印信息的安全性，**防止数据泄露和篡改，确保数据的安全传输和存储。**

02 7.2.1 水印信息预处理

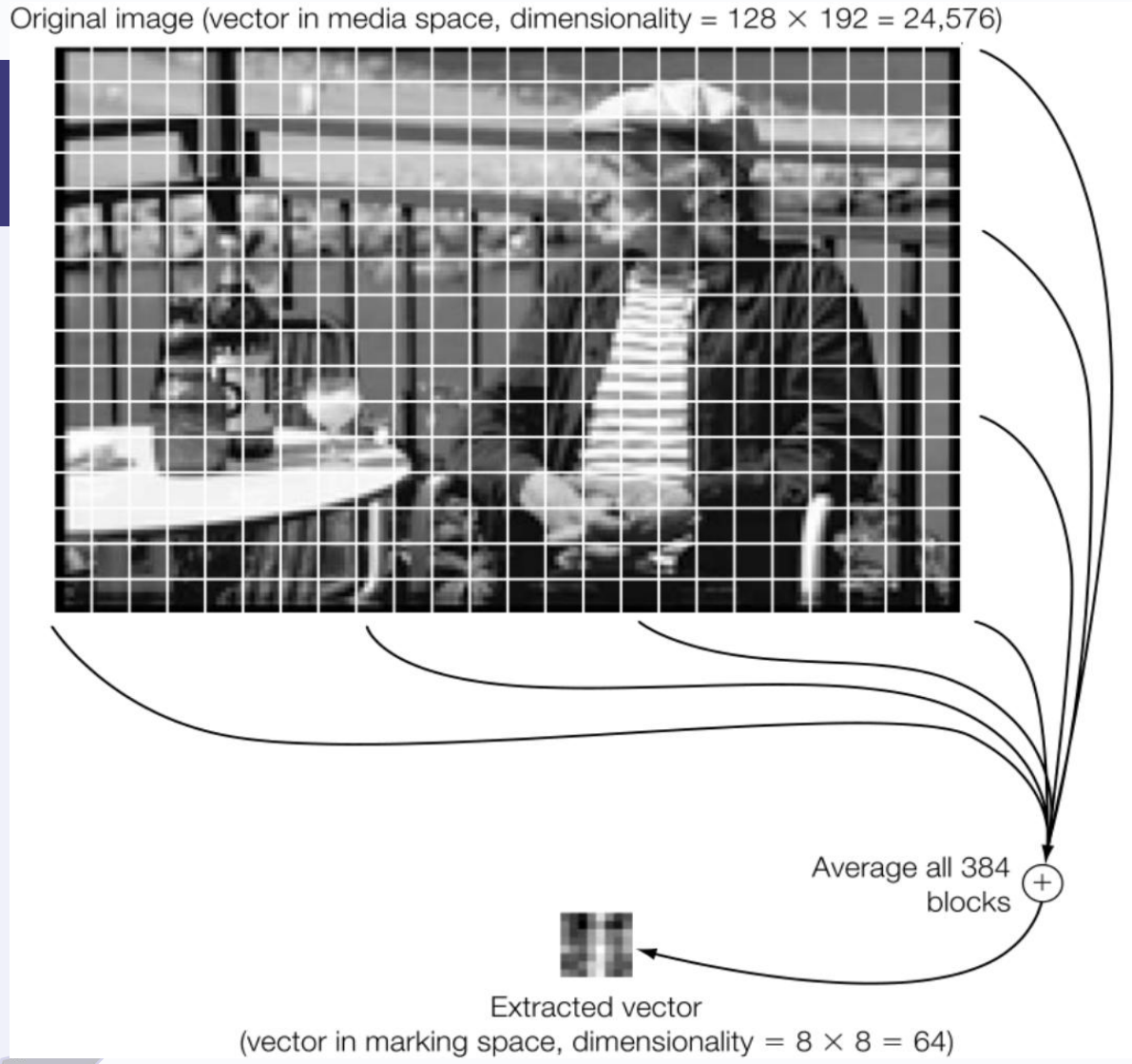
水印信息加密

数据压缩是对水印信息进行处理的关键步骤之一，其目的在于减少数据量并提高嵌入效率。通过数据压缩，可以有效地减少水印信息的存储空间和传输带宽，同时提高水印嵌入和提取的效率。

数据压缩的优势主要体现在以下几个方面：

减少数据量：压缩后的水印信息占用更少的存储空间，降低了数据传输和存储的成本。

提高嵌入效率：压缩后的数据量更小，嵌入到原始数据中的过程更加高效，加快了水印嵌入和提取的速度。



02 7.2.2 水印嵌入算法

空域水印嵌入算法

空域水印嵌入算法直接在数据的原始空间中进行操作，例如在图像的像素值或音频的采样值上进行修改。这种方法简单直接，但通常鲁棒性较差，容易受到各种操作的影响，如压缩、裁剪和噪声添加。

最低有效位

基本原理：将水印信息嵌入到图像像素的最低有效位中。例如，图像的每个像素通常由8位表示，可以将水印信息嵌入到最低位。

优点：实现简单，对图像质量影响较小。

缺点：鲁棒性较差，容易被检测和破坏。

空间编码法

基本原理：通过特定的空间编码方式将水印嵌入到图像中，例如通过修改像素的排列方式。

优点：可以在不显著改变图像的前提下嵌入水印。

缺点：实现复杂度较高，鲁棒性依然有限。

02 7.2.2 水印嵌入算法

空域水印嵌入算法

以下是空域水印嵌入算法的详细步骤：

1.选择嵌入位置：

在原始数据中选择合适的位置进行水印信息的嵌入。选择的位置应该具有足够的容量来嵌入水印信息，并且对原始数据的质量影响较小。常见的选择包括图像的像素值、文本的字符等。

2.水印信息编码：

将要嵌入的水印信息进行编码，以便嵌入到原始数据中。编码过程通常包括将水印信息转换为二进制形式，以便后续嵌入。

3.嵌入水印信息：

在选定的嵌入位置中，将编码后的水印信息嵌入到原始数据中。在图像中，可以通过修改像素的RGB值或灰度值来嵌入水印信息；在文本中，可以通过修改字符的一些属性或位置来嵌入水印信息。

02 7.2.2 水印嵌入算法

空域水印嵌入算法

主要步骤如下：

计算嵌入位置的容量：确定选定位置可以容纳的水印信息的大小，确保不会造成数据溢出。

水印信息与原始数据的融合：根据选定位置的特点，将水印信息与原始数据进行融合。这可以是简单的替换、修改像素值的操作，也可以是更复杂的嵌入算法。

调整嵌入参数：根据需要，调整嵌入的参数，如嵌入强度、密度等，以达到更好的嵌入效果。

4.验证水印嵌入：

在完成水印嵌入后，需要对嵌入后的数据进行验证，以确保水印信息已经成功地嵌入到原始数据中，并且不会对数据的质量产生明显影响。这可以通过提取嵌入的水印信息，并与原始水印进行比较来实现。

02 7.2.2 水印嵌入算法

空域水印嵌入算法

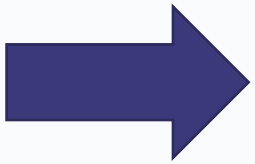
LSB（Least Significant Bit）[6]替换是一种常见且简单的技术，用于将水印信息嵌入到原始数据中。LSB替换的基本思想是将原始数据中最不重要的比特位替换为水印信息，从而在视觉上不影响原始数据的质量，但可以隐藏水印信息。LSB算法利用了数字图像在人眼中的灵敏度有限的特点，通过微小地修改图像像素的最低位来隐藏信息。由于人眼对最低位的变化不敏感，因此修改后的图像在视觉上几乎无法与原始图像区分开来。

原始图像

82	82	82	83
81	82	83	84
82	82	84	86
81	82	83	85

水印图像

1	1	1	1
1	1	0	0
1	0	0	1
1	0	0	1



83	83	83	83
81	83	82	84
83	82	84	87
81	82	82	85

02 7.2.2 水印嵌入算法

LSB优缺点

优点：

简单易实现：LSB替换算法相对简单，易于实现。

隐蔽性较好：由于替换的比特位对原始数据的影响较小，因此水印相对隐蔽，不易被发现。

缺点：

容易受到攻击：LSB替换算法容易受到攻击，例如直方图分析、噪声添加等攻击会破坏水印的鲁棒性。

嵌入容量有限：由于只替换了最不重要的比特位，嵌入的水印容量有限，不能携带大量的信息。

如果嵌入强度过高，可能会导致原始数据的失真，影响数据质量。

LSB替换算法在一些简单场景下仍然具有一定的应用价值，但在对水印鲁棒性和嵌入容量要求较高的情况下，通常需要结合其他更复杂的水印嵌入算法。

02 7.2.2 水印嵌入算法

频域水印嵌入算法

频域水印嵌入算法通过对数据进行变换（如离散傅里叶变换、离散余弦变换、小波变换等），在变换后的频域系数上嵌入水印。这种方法通常鲁棒性较好，能够抵抗各种操作，但实现较为复杂。

离散余弦变换

基本原理：对图像进行DCT变换，将图像从空间域转换到频域，然后在中频或高频系数上嵌入水印，最后进行逆DCT变换恢复图像。

优点：鲁棒性较好，能够抵抗JPEG压缩等操作。

缺点：实现较复杂，计算量大。

离散傅里叶变换

基本原理：对图像进行DFT变换，将图像从空间域转换到频域，然后在频域系数上嵌入水印，最后进行逆DFT变换恢复图像。

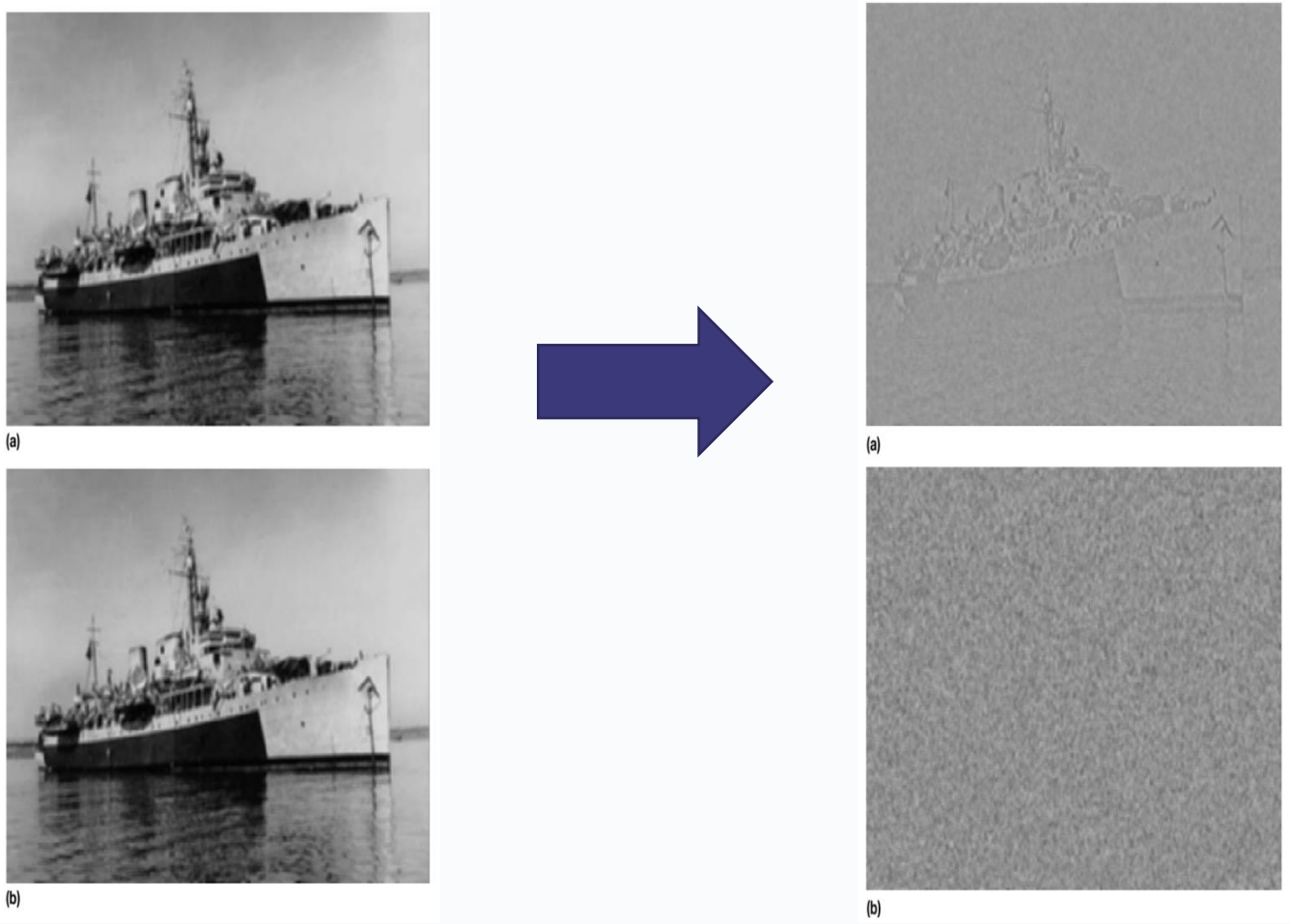
优点：鲁棒性好，能够抵抗旋转、缩放等几何变换。

缺点：计算量大，实现复杂。

02 7.2.2 水印嵌入算法

DCT频域水印嵌入算法

DCT算法是一种常用的频域水印嵌入方法。它将图像分块，并对每个块进行DCT变换。然后，在DCT系数域中嵌入水印信息，通常是修改低频系数。由于DCT变换的能量集中在低频区域．因此在低频系数中嵌入水印可以提高水印的鲁棒性。



02 7.2.2 水印嵌入算法

DCT频域水印嵌入算法

以下是频域水印嵌入算法的基本步骤：

1.频域转换：将原始数据转换到频域表示，常用的转换方法包括傅立叶变换（Fourier Transform）和离散余弦变换（Discrete Cosine Transform，DCT）。这些变换将数据从时域（时间域）转换到频域（频率域），使得数据的特征以频率分布的形式呈现。

2.水印信息编码：将要嵌入的水印信息进行编码，通常将其转换为频域表示以便与原始数据进行合并。水印信息的编码过程可能需要考虑到频域转换后的特性，以确保嵌入后的水印能够在提取时被准确识别。

3.选择嵌入位置：在频域表示中选择合适的位置嵌入水印信息。这通常需要考虑到频域系数的敏感性和鲁棒性，以及对原始数据的影响程度。

4.嵌入水印信息：将编码后的水印信息嵌入到选定的频域位置中。嵌入的方式可以是简单的加法、乘法或修改频域系数的幅度和相位等。

5.逆频域转换：将嵌入了水印信息的频域数据转换回时域表示，恢复原始数据的格式和结构。

6.验证嵌入效果：在完成水印嵌入后，需要对嵌入后的数据进行验证，以确保水印信息已经成功地嵌入到原始数据中，并且对数据的质量影响较小。

频域水印嵌入的重点算法包括频域转换算法、水印信息编码算法、嵌入位置选择算法、嵌入策略设计算法和嵌入效果验证算法。这些算法共同构成了频域水印嵌入的核心，通过合理选择和设计这些算法，可以实现对数据的有效保护和管理。

第7章 数据安全概述

本讲内容概要：

01 第一节—数据水印基本原理

02 第二节—数据水印嵌入

03 第三节—数据水印提取

04 第四节—数据水印应用

03 7.3 水印检测概念

数据水印提取是指从包含水印的数字媒体中检测、识别和提取水印信息的过程。这一过程是数字水印技术的关键环节之一，允许合法的用户或系统从嵌入了水印的媒体中提取出水印信息，以进行身份验证、版权保护、内容认证等应用。

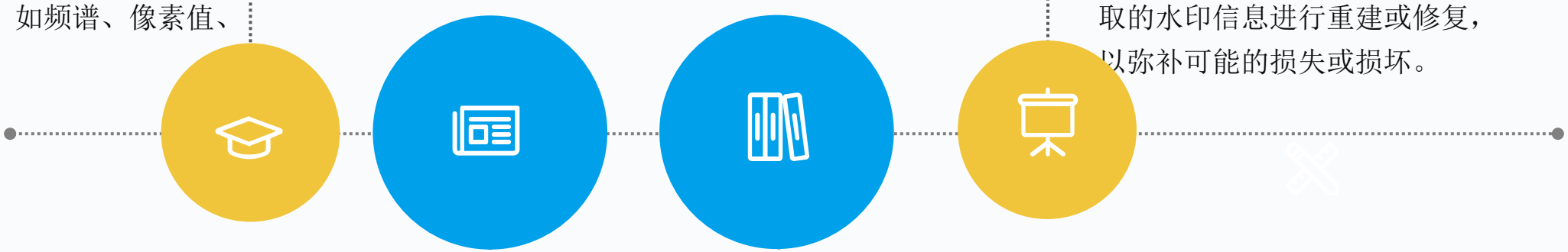
在数据水印提取过程中，通常会使用特定的提取算法或技术来分析嵌入了水印的数字媒体，并从中提取出水印信息。取根据提取时已知信息的多少，**分为盲水印提取、非盲水印提取以及混合水印提取方法。**

数据水印提取的结果通常是原始水印或水印相关的信息，可以被用于不同的应用场景。例如，在版权保护方面，提取出的水印信息可以用于验证数字内容的所有权；在内容认证方面，水印信息可以用于验证数字内容的完整性和真实性；在数字取证方面，水印信息可以用于追踪和证实数字证据的来源和真实性。

03 7.3.1 检测基本原理

特征提取

首先，从包含水印的数字媒体中提取出可能与水印相关的特征。这些特征可能包括图像、音频、视频或文本等不同媒体类型的特征，如频谱、像素值、字节序列等。



水印检测

通过分析提取的特征，检测数字媒体中是否存在水印。这可能涉及使用特定的检测算法或技术来识别水印的存在，例如，检测图像中像素值的微小变化或音频中频谱的异常。

水印提取

一旦水印被检测到，接下来是从数字媒体中提取水印信息。这通常涉及使用特定的提取算法或技术，根据水印的嵌入方式和特征来恢复原始的水印息。

验证和重建

提取的水印信息可能需要经过验证以确保准确性和完整性。在一些情况下，可能需要对提取的水印信息进行重建或修复，以弥补可能的损失或损坏。

03 7.3.2 盲水印提取

统计特征方法

统计特征方法利用数据的统计特性进行水印提取。它们通常不依赖于原始数据，可以在修改后的数据中提取水印。

特征域方法

特征域方法通过提取数据中的特征信息来嵌入和提取水印。这些特征信息通常是数据的局部特征，如边缘、纹理等。

信息论方法

信息论方法利用信息论的概念，如熵、互信息等进行水印的嵌入和提取。这类方法关注数据的信息含量和传输效率。

盲水印提取

盲水印提取是指在不需要原始未嵌入水印的数据或任何先验信息的情况下，从被嵌入水印的数据中提取出水印信息的过程。这种方法非常适用于实际应用，因为在很多情况下，原始数据可能并不可用。

03 统计特征方法

基于统计特征的方法是一种盲水印提取方法，它利用图像的统计属性来提取水印信息，而无需访问原始水印信息。这些统计属性通常包括图像的平均值、方差、相关系数等。

具体来说，统计特征的方法包括以下步骤：

1. 统计分析：首先对载体图像进行统计分析，了解其特性和可能存在的水印变化。这可能包括分析图像的像素值分布、颜色空间、频谱特征等。

2. 水印检测：基于对载体图像的统计分析，识别可能存在的水印信号。这可以通过比较载体图像的特定统计特征（如平均值、方差等）与预期的水印特征进行实现。

03 统计特征方法

基于统计特征的方法是一种盲水印提取方法，它利用图像的统计属性来提取水印信息，而无需访问原始水印信息。这些统计属性通常包括图像的平均值、方差、相关系数等。

具体来说，统计特征的方法包括以下步骤：

3. 提取过程：一旦检测到可能的水印信号，接下来是通过统计特征的变化来确定水印的存在与否以及水印的内容。提取过程可能包括提取图像的平均值、方差等统计特征，并与未嵌入水印的图像进行比较。

4. 水印提取：根据比较结果，提取隐藏在图像中的水印信息。这可能需要进一步的分析和处理，以确定水印的完整性和正确性。

03 统计特征方法

基于统计特征的盲水印提取方法具有以下特点：

无需原始水印信息：不需要访问原始水印信息即可提取水印，因此更加安全可靠。

简单高效：提取过程相对简单，只需要对图像的统计特征进行分析和比较，因此实现起来比较容易。

适用范围广：适用于各种类型的数字媒体，包括图像、音频、视频等，因为统计特征在不同类型的媒体中都是普遍存在的。

鲁棒性较强：对于一定程度的图像变换和攻击具有一定的鲁棒性，可以保持一定的提取准确性。

对图像变换敏感：虽然具有一定的鲁棒性，但仍然对图像的一些变换敏感，例如压缩、旋转等操作可能会影响提取的准确性。

03 特征域方法

特征域方法[11]是一种常用的数字水印提取算法，它利用数字媒体在特定域（如频域、空域等）中的特征来提取水印信息。这种方法通常涉及对数字媒体进行变换或分析，以突出水印嵌入的特征，并通过相应的处理方法将水印提取出来。

03 特征域方法

特征域方法在数字水印提取中具有以下几个特点：

适用性广泛：特征域方法适用于各种不同类型的数字媒体，包括图像、音频、视频等，以及各种不同类型的水印。这种方法可以根据具体的媒体和水印特性选择合适的特征域和处理方法，因此具有较广泛的适用性。

高提取性能：特征域方法能够从数字媒体中有效地提取出水印信息。通过在特征域中突出水印的特征并进行相应的处理，这种方法能够在不损失水印信息质量的情况下实现高效的水印提取。

抗攻击能力：特征域方法通常具有一定的抗攻击能力，能够在一定程度上抵抗常见的攻击，如压缩、旋转、加噪声等。这是因为水印通常会以特定的方式嵌入到数字媒体的特征域中，使得水印在受到一些常见攻击时仍然能够被有效提取。

灵活性：特征域方法具有较高的灵活性，能够根据具体的应用需求和水印特性选择合适的特征域和处理方法。这使得该方法在不同的应用场景和媒体类型下都能够灵活地应用，并取得良好的效果。

理论基础强：特征域方法通常建立在坚实的数学和信号处理理论基础之上，如傅立叶变换、小波变换等。这些理论基础能够有效地支撑特征域方法的实现和优化，使其具有更好的水印提取性能和可靠性。

03 信息论方法

信息论方法是一种基于信息论原理和技术的数字水印提取方法。信息论是研究信息传输、存储和处理的数学理论，其主要研究对象是信息的量、传输和存储的效率等。在数字水印领域，信息论方法利用信息论的相关概念和方法，通过对数字媒体和水印之间的统计关系进行建模和分析，实现水印信息的提取。

信息论方法的主要思想是利用数字媒体和水印之间的统计特性，通过数学建模和推导提取算法来实现对水印信息的提取。这种方法通常涉及到对数字媒体和水印的概率分布、相关性等进行建模，并利用信息论的相关理论和方法推导出最优的水印提取算法。信息论方法通常能够在不依赖额外信息的情况下，从数字媒体中提取出水印信息，具有一定的抗攻击能力和提取性能。

03 信息论方法

信息论方法的基本步骤如下：

1. 建立数学模型：首先，需要对数字媒体和水印之间的统计关系进行数学建模。这包括分析数字媒体的统计特性、水印的嵌入方式以及可能的攻击模型等。建立良好的数学模型是信息论方法的基础，它为后续的水印提取算法设计提供了理论支持。

2. 推导提取算法：基于建立的数学模型，可以使用信息论的相关理论和方法推导出水印提取的最优算法。这可能涉及使用最大似然估计、条件熵最小化等统计方法来设计提取算法，从而实现对水印信息的有效提取。

3. 优化设计：设计提取算法时需要考虑到数字媒体可能存在的各种噪声和干扰，以及可能的攻击模型。因此，需要对提取算法进行优化设计，使其能够在噪声环境和攻击条件下保持较高的提取性能和鲁棒性。

4. 实现和验证：设计好的提取算法需要进行实际的实现和验证。这可能涉及使用计算机编程语言实现提取算法，并对其进行测试和验证，以确保算法能够在实际应用中有效地提取出水印信息。

03 7.3.3 非盲水印提取

差分法

基本原理：通过对比嵌入水印的数据与原始数据之间的差异来提取水印

变换域方法

基本原理：在频域或其他变换域中，将嵌入水印的数据与原始数据进行对比，提取出水印。

叠加法

基本原理：将嵌入水印的数据与原始数据叠加，通过叠加结果提取水印信息。

非盲水印提取

非盲水印提取是一种在提取水印时需要原始数据或先验信息的方法。与盲水印提取相比，非盲水印提取方法在准确性和鲁棒性上具有优势。常见的非盲水印提取方法包括差分法、相减法、变换域方法和叠加法等。选择具体方法时，需要考虑数据类型、嵌入方法和应用需求，以实现最佳的提取效果。

03 7.3.4 混合水印提取

多层次水印提取

在数据中嵌入多层次的水印信息，每层次使用不同的提取方法

混合域水印提取

结合空域和频域的水印提取方法，提高水印提取的鲁棒性和准确性。

联合检测法

同时使用盲检测和非盲检测方法，对提取结果进行联合验证和综合判断

混合水印提取

混合水印提取方法结合了盲水印提取和非盲水印提取的优点，具有灵活性强、适用范围广和高鲁棒性的特点。常见的混合水印提取方法包括多层次水印提取、混合域水印提取、自适应混合水印提取和联合检测法等。选择具体方法时，需要根据数据类型、嵌入方法和实际需求，灵活应用不同的提取技术，以实现最佳的提取效果

第7章 数据安全概述

本讲内容概要：

01 第一节—数据水印基本原理

02 第二节—数据水印嵌入

03 第三节—数据水印提取

04 第四节—数据水印应用

04 7.4 数据水印应用

版权保护

版权保护是一种重要的知识产权保护措施，旨在保护作者或创作者的原创作品免受未经授权的复制、传播或修改。

身份验证

身份验证是确认一个个体或实体是否真实、合法或可信的过程，通常通过检查、验证和确认其所提供的身份信息或特征来实现。

内容追踪

内容追踪是指监控和跟踪数字内容在互联网上的传播、使用和分享情况的过程。这种追踪可以通过技术手段来实现，例如数据水印、数字版权管理系统等，

隐私保护

隐私保护是指保护个人身份、个人信息和私人活动免受未经授权的访问、使用或泄露的过程。

04 7.4.1 版权保护

版权保护是一种重要的知识产权保护措施，旨在保护作者或创作者的原创作品免受未经授权的复制、传播或修改。这包括文学作品、音乐、艺术品、软件、电影和其他创意作品等各种形式的创作。

软件版权保护

应用范围：各种类型的软件和应用程序。

实现方式：在软件代码或资源文件中嵌入版权信息，防止盗版和未经授权的使用。

提取与验证：通过提取嵌入的水印信息来验证软件的正版性和版权归属。

04 7.4.1 版权保护

版权保护是一种重要的知识产权保护措施，旨在保护作者或创作者的原创作品免受未经授权的复制、传播或修改。这包括文学作品、音乐、艺术品、软件、电影和其他创意作品等各种形式的创作。

数字媒体的版权保护

应用范围：图像、音频、视频、文本等数字媒体内容。

实现方式：在数字媒体文件中嵌入版权信息（如版权声明、版权所有者标识、版权日期等）。

提取与验证：在发生版权纠纷或侵权行为时，通过提取嵌入的水印信息来确认和验证版权归属。

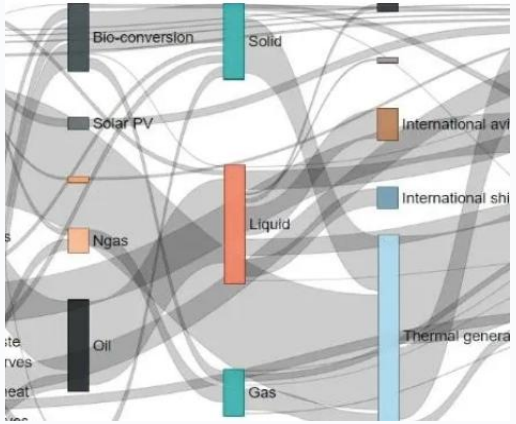
04 7.4.2 身份验证

身份验证是确认一个个体或实体是否真实、合法或可信的过程，通常通过检查验证和确认其所提供的身份信息或特征来实现。这种过程可以包括使用各种手段和技术，如密码、生物特征识别、数字签名等，以确保只有授权的用户才能访问敏感信息、系统或资源。

数字图像认证：在数字图像中嵌入水印可以用于验证图像的来源和真实性。例如，摄影师可以在其摄影作品中嵌入数字签名或特定标识，以证明图像的原创性和版权归属。

身份证明文件：在数字身份证明文件（如电子身份证、护照等）中嵌入水印可以用于验证文件的真实性和完整性。水印可以包括个人身份信息、发行机构信息等，以提供额外的身份验证信息。

04 7.4.3 内容追踪



内容追踪是指监控和跟踪数字内容在互联网上的传播、使用和分享情况的过程。这种追踪可以通过技术手段来实现，例如数据水印、数字版权管理系统等，以及通过监控和分析网络数据流量、用户行为和社交媒体平台等方式。

数字媒体追踪：在数字媒体（如图像、音频、视频等）中嵌入水印可以用于追踪其在网络上的传播和使用情况。这对于版权保护、内容监控和违规行为的检测都非常有用。通过检测水印，可以确定数字内容的原始来源和传播路径。

防止盗版和非法传播：数字媒体常常受到盗版和未经授权的复制的威胁。通过在数字内容中嵌入水印，可以追踪其传播路径，并及时发现和阻止非法传播行为，从而保护内容创作者的权益。

04 7.4.4 隐私保护

隐私保护是指保护个人身份、个人信息和私人活动免受未经授权的访问、使用或泄露的过程。

匿名化数据：在敏感数据或个人身份信息中嵌入水印可以帮助匿名化数据，以保护个人隐私。**数据共享安全：**在共享数据时，嵌入水印可以帮助追踪数据的使用和传播，从而确保数据的安全性和隐私性。水印可以标识数据的来源和访问者身份。

谢谢！